Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional): NAI1P361/00.166.01

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on May 31, 2006

Signature: [signature]

Typed or printed name: Erica L. Farlow

Application Number	Filed
09/803,527	03/08/2001

First Named Inventor: M. McArdle et al.

Art Unit	Examiner
2145	Choudhury, A.

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

- [ ] applicant/inventor.
- [ ] assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- [x] attorney or agent of record. Registration number 41,429
- [ ] attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____

[signature]
Signature

Kevin J. Zilka
Typed or printed name

(408) 971-2573
Telephone number

05/30/06
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

- [ ] *Total of _____ forms are submitted.

REMARKS

The Examiner has rejected Claims 1-21, 24-32 and 41-43 under 35 U.S.C. 103(a) as being unpatentable over Coss et al. (U.S. Patent No. 6,098,172) in view of Minear et al. (U.S. Patent No. 5,983,350). Applicant respectfully disagrees with such rejection.

With respect to each of the independent claims, the Examiner has relied on Col. 6, lines 49-67 from the Coss reference to make a prior art showing of applicant's claimed technique "wherein the security policy section specifies filters for at least a portion of ports and services defined by the network protocol, and each port and service associated with the security policy is identified by an element identifier field, a field containing filter settings, and a log indicator field" (see this or similar, but not necessarily identical language in each of the independent claims). Applicant's arguments made in Amendment D mailed 03/31/2006 on page 11, third paragraph – page 12, second paragraph are incorporated by reference.

Further, in the Advisory Action mailed 04/24/2006, the Examiner argued that the "Service," "Source Host," "Destination Host," "Audit Session," and "Action" categories in the chart listed in between Cols. 3 and 4 in Coss disclose the aforementioned claimed features. Applicant respectfully disagrees. Specifically, Coss discloses that "[t]he security policies can be represented by sets of access rules which are represented in tabular form." However, the sets of access rules in the security policy fail to meet a technique "wherein the security policy section specifies filters for at least a portion of ports and services defined by the network protocol, and each port and service associated with the security policy is identified by an element identifier field, a field containing filter settings, and a log indicator field" (emphasis added), as claimed by applicant. Moreover, applicant asserts that the "Action" category field with the description of '[r]ule action, e.g., "pass," "drop" or "proxy",' as cited by the Examiner, simply fails to disclose "a field containing filter settings," as claimed by applicant.

Further, with respect to each of the independent claims, the Examiner has relied on Claim 8 from the Minear reference to make a prior art showing of applicant's claimed technique "wherein a security policy section of the policy file data structure includes an entry

for each security policy that is identified by a policy identifier field and is associated with a network protocol that is identified by a protocol identifier field" (see this or similar, but not necessarily identical language in each of the independent claims). Applicant's arguments made in Amendment D mailed 03/31/2006 on page 12, third paragraph – page 13, second to last paragraph are incorporated by reference.

Additionally, the Examiner has not even specifically addressed applicant's claimed technique "wherein at least one security policy is included for a TCP/IP network and includes a PPTP (point-to-point tunneling protocol), a RIP (routing information protocol), a DHCP (dynamic host configuration protocol), an ARP (address resolution protocol), an Ident (identification protocol), ICMP (internet control message protocol) and VPN (virtual private networking) ports, and a NetBIOS (network basic input/output system) service;" "wherein a zone section of the policy file data structure includes an entry for each defined address zone and includes an identifier field, an address parameters field that defines the zone, and an identifier field for the security policy assigned to the zone;" "wherein a default zone is defined by addresses that are outside another zone;" and "wherein the security policy associated with the network protocol is specific to the network protocol." After careful review of both the Minear and Coss references, applicant notes that the above language claimed by applicant is clearly not even suggested by the prior art of record.

In the Advisory Action mailed 04/24/2006, the Examiner argued "that no limit is placed by either art as to what types of protocols can be handled within the firewall designs" and that "claim 8 of Minear's design demonstrates how multiple protocols are applicable to the design." Applicant respectfully disagrees with such argument, in that it is improper to rely on open ended, ambiguous prior art disclosures to reject applicant's specific claimed features. Miner's disclosure simply does not rise to the level of specificity of applicant's claim limitations.

Specifically, applicant respectfully asserts that each "network protocol stack connected to [a] communications interface," as disclosed by Minear in claim 8, simply fails to meet a technique "wherein at least one security policy is included for a TCP/IP network

and includes a PPTP (point-to-point tunneling protocol), a RIP (routing information protocol), a DHCP (dynamic host configuration protocol), an ARP (address resolution protocol), an Ident (identification protocol), ICMP (internet control message protocol) and VPN (virtual private networking) ports, and a NetBIOS (network basic input/output system) service" (emphasis added), as claimed by applicant.

Furthermore, with respect to the independent claims, the Examiner has simply dismissed, under Official Notice, applicant's claimed techniques "wherein the security policy is defined by a policy file which includes a policy file data structure stored as an XML (extensible markup language) document" and "wherein a default setting for a high security policy on the TCP/IP network disallows incoming network traffic through the PPTP and ICMP ports, allows incoming network traffic through the RIP, DHCP, ARP and VPN ports, disallows access through the NetBIOS service to shared resources on the individual computer, and disallows the individual computer from using shared resources of other computers on the TCP/IP network, where incoming network traffic that attempts to access the individual computer using PPTP and NetBIOS is logged" under Official Notice. Applicant's arguments made in Amendment D mailed 03/31/2006 on page 14, last two paragraphs are incorporated by reference.

In the Advisory Action mailed 04/24/2006, the Examiner, in a blanket manner, citied Greschler et al. (U.S. Patent No. 6,938,096) to make a prior art showing of such claimed features. Applicant has reviewed the entire Greschler reference and asserts that Greschler fails to disclose a technique "wherein a default setting for a high security policy on the TCP/IP network disallows incoming network traffic through the PPTP and ICMP ports, allows incoming network traffic through the RIP, DHCP, ARP and VPN ports, disallows access through the NetBIOS service to shared resources on the individual computer, and disallows the individual computer from using shared resources of other computers on the TCP/IP network, where incoming network traffic that attempts to access the individual computer using PPTP and NetBIOS is logged," as claimed by applicant. Applicant respectfully requests a specific prior art reference citation that discloses such claimed features, or a notice of allowance.

In the Advisory Action mailed 04/24/2006, the Examiner, again, in a blanket manner, cited Stiles et al. (U.S. Patent No. 6,842,737), Virgin et al. (U.S. Patent No. 6,826,542), and MacPhail (U.S. Patent No. 6,593,943). Applicant has carefully considered the references relied upon by the Examiner, and asserts that they merely teach usage of XML documents. The references simply fail to disclose a technique "wherein the security policy is defined by a policy file which includes a policy file data structure stored as an XML (extensible markup language) document" (emphasis added), as claimed by applicant. Again, applicant respectfully requests a specific prior art reference citation that discloses such claimed features, or a notice of allowance.

Further, with respect to such subject matter of former Claim 5 (now at least substantially incorporated into each of the independent claims), the Examiner has relied on Col. 7, lines 61-67 from the Coss reference, along with Claim 8 from the Minear reference (reproduced above), to make a prior art showing of such claimed feature. Applicant's arguments made in Amendment D mailed 03/31/2006 on page 16, first three paragraphs are incorporated by reference.

In the Advisory Action mailed 04/24/2006, the Examiner argued that Fig. 5A in Coss "indicated the comparison of address versus a table" and that Fig. 7 in Coss "indicates how the address range is considered and an appropriate response is performed based on the address range." Specifically, Fig. 5 indicates a yes/no branch if the "domain [is] in [the] table," and Fig. 7 indicates a yes/no branch if the "packet address [is] within range." The branches indicated in the referenced figures clearly fail to disclose a technique "wherein the zone is defined by a set of network addresses, which comprises at least one address outside the zone" (emphasis added), as claimed by applicant.

In addition, with respect to the subject matter of former Claims 41, 42, and 43 (now at least substantially incorporated into each of the independent claims in Markush-type format), the Examiner has relied Col. 9, lines 6-9 from the Coss reference, along with Claim 8 from the Minear reference, to make a prior art showing of applicant's claimed techniques.

Applicant's arguments made in Amendment D mailed 03/31/2006 on page 14, last paragraph – page 15, last paragraph are incorporated by reference.

In the Advisory Action mailed 04/24/2006, the Examiner, in a blanket manner, relied upon NETBIOS RFC 1001, MANET RFC 2501, and DHCP RFC 2131 to make a prior art showing of such claimed features. Specifically, page 10 of NETBIOS RFC 1001 discloses that "NetBIOS resources are referenced by name" and that "an application, representing a resource, registers one or more names that it wishes to use." However, referencing a resource by name simply fails to disclose a technique "wherein the network address dynamically assigned to the network adapter is determined by mapping an adapter registry identifier to an associated network address stored in an operating system registry" (emphasis added), as claimed by applicant. In addition, pages 4 and 5 of MANET RFC 2501 disclose that '[t]he concept of a "node identifier" (separate and apart from the concept of an "interface identifier") is crucial to supporting the multigraph topology of the routing fabric.' MANET continues to disclose that this node identifier "is what *unifies* a set of wireless interfaces and identifies them as belonging to the same mobile platform [which] permits maximum flexibility in address assignment." However, the node identifiers as disclosed in MANET simply fail to even suggest a technique "wherein the network address dynamically assigned to the network adapter is determined by monitoring network traffic at the network adapter and examining a predefined limited amount of the network traffic to determine the network address" (emphasis added), as claimed by applicant. Furthermore, pages 12 and 15 of DHCP RFC 2131 teach that "[t]he client broadcasts a DHCPDISCOVER message on its local physical subnet" and "[t]he server selected in the DHCPREQUEST message commits the binding for the client to persistent storage and responds with a DHCPACK message containing the configuration parameters for the requesting client." However, this client request and server response fails to disclose a technique "wherein the network address dynamically assigned to the network adapter is determined by receiving a network address from a network adapter device driver when the network adapter connects to the TCP/IP network" (emphasis added), as claimed by applicant.